PACIFIC JOURNAL OF MATHEMATICS
Vol. 23, No. 3, 1967

POLYNOMIALS IN CENTRAL ENDOMORPHISMS

FRANKLIN HAIMO

Let λ be a central endomorphism of a group G in the sense that λ induces the identity map on the inner automorphism group of G. Despite the nearness of the situation to commutativity, it is not necessarily true that the central endomorphisms of G form a ring or even that the subset generated by λ be a ring. The displacement map τ, given by $\tau(g) = g^{-1}\lambda(g)$ for each $g \in G$, is an endomorphism with central values. We shall show (Theorem 1) that if τ satisfies a certain pair of simultaneous equations then λ or λ^2 is idempotent. Let P be a formal polynomial with integral coefficients, and let t be the sum of these coefficients. Then (Theorem 2) $P(\lambda)$ is an endomorphism if and only if t induces an integral endomorphism on G. If G is nilpotent of class 2 then (Theorem 3) $P(\lambda)$ is an endomorphism if and only if $t(t-1)/2$ is an exponent for the commutator subgroup Q of G.

Theorem 3 gives us an alternate proof of an older (essentially equivalent) result [2, Th. 7, Corollary]. If α and β are two maps in G^G, then $\gamma = \alpha + \beta$ is to mean the map given by $\gamma(g) = \alpha(g)\beta(g)$ for all $g \in G$. The symbol ι will be reserved for the identity map on G. By $\operatorname{diag}_m x$ we mean the m-by-m matrix with x repeated down the main diagonal and with zeros elsewhere. If 1_G is the unity of the group G, we say that an integer m is an exponent of G if $g^m = 1_G$ for each $g \in G$. An integer m is said to induce an integral endomorphism on a group G if $(xy)^m = x^m y^m$ for all $x, y \in G$.

1. Preliminaries. Let τ be a center-endomorphism of a group G. That is, τ is an endomorphism of G, and $\operatorname{Im}\tau \leqq Z$, the center of G. The map $\lambda \in G^G$ given by $\lambda(x) = x\tau(x)$ for each $x \in G$ is a normal endomorphism of G in that it commutes with each inner automorphism of G. It is a central endomorphism in that $\lambda = \iota + \tau$ where τ is a center-endomorphism. See [3]. Each center-endomorphism of G is likewise a normal endomorphism; but if G is nonabelian, no such endomorphism is a central endomorphism. The central endomorphism $\lambda = \iota + \tau$ is said to be related to the center-endomorphism τ. The set of all center-endomorphisms of a group G is a ring $C(G)$ under endomorphism addition and composition.

If τ is a center-endomorphism of G with related central endomorphism λ, then, with multiplication proceeding from left to right with increasing i and with $C(n, i)$ as the usual binomial coefficient, we have

$$(A_n) \qquad \lambda^n(x) = x \prod_{i=1}^{n} \tau^i(x^{C(n,i)})$$

and

$$(B_n) \qquad \tau^n(x) = \left[x \prod_{i=1}^{n} \lambda^i(x^{(-1)^i C(n,i)}) \right]^{(-1)^n}$$

for each $x \in G$ and for each positive integer n. From (A_n), each λ^n is a central endomorphism related to $\sum_{i=1}^{n} C(n, i)\tau^i \in C(G)$ where λ is related to τ. One readily sees that λ is idempotent if and only if $-\tau$ is idempotent. Under this assumption, $\tau^{2j+1} = \tau = -\tau^{2j}$ for each positive integer j.

Observe that the 2^n factors on the right of (B_n) can be rearranged at will. In fact, if one considers the mapping $P(\lambda) = \sum_{i=0}^{n} a_i\lambda^i$ where the a_i are integers with $a_n \neq 0$, where $\lambda^0 = \iota$, and where $P(\lambda)x = \prod_{i=0}^{n} \lambda^i(x^{a_i})$ for each $x \in G$, then the terms of $P(\lambda)$ can be rearranged in any way. Nevertheless, $P(\lambda)$ need not be an endomorphism. If, however, it is an endomorphism, then it is normal. Call n the degree of P.

THEOREM 1. *Let τ be a center-endomorphism with related central endomorphism λ on a group G.*

(a) *Suppose that there exist integers $m > 0$ and $k \geqq 0$ such that $\tau^{2m+k} + \tau^m = 0$. Then there exists a formal polynomial P with integral coefficients and of degree $2m + 2k$ for which λ is a zero.*

(b) *If there exists an integer $n \geqq 3$ such that $\tau + \tau^{n-1} = 0 = \tau^2 + \tau^{n-2}$, then λ is idempotent if n is odd; while if n is even, $\operatorname{Im}\tau$ is elementary 2-abelian, $\lambda^3 = \lambda^2$, and λ^2 is idempotent.*

Proof. (a) From $\tau^{2m+2k} + \tau^{m+k} = 0$ and the above remark on idempotents, the central endomorphism σ related to τ^{m+k} must be idempotent. From (B_{m+k}), σ must be of degree $m + k$ as a polynomial in λ. Let T be the formal polynomial corresponding to σ. Let $P = T^2 - T$.

(b) $\tau = \tau^3$ so that $\tau^2 = \tau^4$, all odd powers reducing to τ, even to τ^2. If n is odd, then $\tau^{n-1} = \tau^2$ while $\tau^{n-2} = \tau$, from which $\tau^2 = -\tau$ and $\lambda^2 = \lambda$. If n is even, $\tau^{n-1} = \tau$ whence $\tau^{n-1} + \tau = 0$ yields $\tau(x^2) = 1_G$ for every $x \in G$. At once, $\operatorname{Im}\tau$ is elementary 2-abelian. Now, (A_2) leads to $\lambda^2(x) = x\tau^2(x)$ in this case. Applying λ, $\lambda^3(x) = x\tau(x^2)\tau^2(x) = \lambda^2(x)$. Thus, $\lambda^3 = \lambda^2$, all higher powers reducing to λ^2. In particular, λ^2 is idempotent.

As an example of (b), take G to be the group of m-by-m non-singular real matrices, and, for each matrix A therein, let $\tau(A) = \operatorname{diag}_m(|\det A|^{-1/m})$. It is clear that τ is a center-endomorphism of G and that $\tau^2 + \tau = 0$. If we take $n = 3$, we have the situation in (b).

2. The sum of the coefficients. If P is a polynomial with integral coefficients, let $t(P)$ denote the sum of these coefficients.

LEMMA. *Let α be a center-endomorphism of a group G, and let β be a member of G^G. Then $\alpha + \beta$ is an endomorphism of G if and only if β is an endomorphism.*

Proof. $(\alpha + \beta)(xy) = \alpha(x)\alpha(y)\beta(xy)$ while $(\alpha + \beta)(x)(\alpha + \beta)(y) = \alpha(x)\beta(x)\alpha(y)\beta(y)$. Since $\alpha(y)$ is in the center, the result is clear.

If k is an integer, let $[k]$ be that member of G^G which is given by $[k]x = x^k$ for each $x \in G$. Observe that if τ is a center-endomorphism of G, then τ generates a subring $\{\tau\}$ of $C(G)$.

THEOREM 2. *Let τ be a center-endomorphism of a group G, and let λ be its related central endomorphism. Let P be a polynomial with integral coefficients.*

(a) *If $t(P) = 0$, then $P(\lambda)$ is a center-endomorphism, a member of $\{\tau\}$.*

(b) *If $t(P) = 1$, then $P(\lambda)$ is a central endomorphism related to some member of $\{\tau\}$.*

(c) *If G is noncommutative and if $t(P) = 2$, then $P(\lambda)$ is no endomorphism.*

(d) *If $t(P) \neq 0, 1, 2$, then $P(\lambda)$ is:* (1) *an endomorphism if and only, if $[t(P)]$ is an endomorphism on G;* (2) *a center-endomorphism if and only if $[t(P)]$ is a center-endomorphism on G;* (3) *a central endomorphism if and only if $[t(P) - 1]$ is a center-endomorphism on G.*

Proof. Suppose that $P(\lambda) = \sum_{i=0}^{n} a_i\lambda^i$ for integers a_i. Note that $\lambda^0 = \iota$ and that, from (A_i), $\lambda^i = \iota + \sum_{j=1}^{i} C(i, j)\tau^j$ if $i > 0$. Upon substitution, $P(\lambda) = \sum_{i=0}^{n} a_i(\iota + \sum_{j=1}^{i} C(i, j)\tau^j) = t(P)\iota + \sum_{i=1}^{n} q_i\tau^i$ for suitable integers q_i. (a) and (b) are now immediate. If $t(P) = 2$, the lemma says that $2\iota = [2]$ is an endomorphism of G if and only if $P(\lambda)$ is an endomorphism. But $[2]$ is an endomorphism if and only if G is abelian, establishing (c). For $t(P) \neq 0, 1, 2$, the lemma gives (d), (1) and (2), directly. Now $P(\lambda)$ is central and related to a center-endomorphism if and only if $P(\lambda) = \iota + \sigma$ for some center-endomorphism σ. Equivalently, $(t(P) - 1)\iota + \sum_{i=1}^{n} q_i\tau^i - \sigma = 0$; that is, $(t(P) - 1)\iota = [t(P) - 1]$ is a center-endomorphism on G, establishing (d), (3).

By (a) above, each $\lambda^n - \lambda$ is a center-endomorphism, $n = 1, 2, \cdots$. By (c), if G is noncommutative, no $\lambda^n + \lambda$ is an endomorphism, $n = 1, 2, \cdots$.

Recall that a group is (nilpotent) of class 2 if its inner automorphism group is abelian.

THEOREM 3. *Let G be a class 2 group, λ a central endomorphism of G, and P a polynomial with integral coefficients. Then $P(\lambda)$ is a normal endomorphism of G if and only if $(t(P) - 1)t(P)/2$ is an exponent of Q.*

Proof. Note that $P(\lambda) = \sum_{i=0}^{n} a_i\lambda^i$ is a normal endomorphism if and only if it is an endomorphism. Each λ^i is central (by A_i). For $x, y \in G$, let w denote $[y^{-1}, x^{-1}] = y^{-1}x^{-1}yx$. For a class 2 group, recall that $y^b x^a = x^a y^b w^{ab}$ and that $(xy)^a = x^a y^a w^{a(a-1)/2}$ for all integers a and b. By the centrality of the powers of λ, $\lambda^i(y^b)\lambda^j(x^a) = \lambda^j(x^a)\lambda^i(y^b)w^{ab}$ for all $x, y \in G$, all nonnegative integers i and j, and all integers a and b. It is now easy to show that $P(\lambda)(xy) = P(\lambda)(x)P(\lambda)(y)w^E$ where the integer $E = \sum_{i=0}^{n} a_i(a_i - 1)/2 + \sum_{i<j} a_i a_j$. From a routine observation one sees that $E = (t(P) - 1)t(P)/2$.

COROLLARY. [2, Th. 7, Corollary] *Let s be an integer $\neq 0, 1, 2$. Let G be a class 2 group for which $s(s-1)/2$ is an exponent for Q. Then $[s]$ is an integral endomorphism for Q.*

Proof. By the theorem, any polynomial P with integral coefficients and with coefficient-sum s has $P(\lambda)$ an endomorphism for each central endomorphism λ, and the set of all such λ is nonempty. By Theorem 2, (d), $[s]$ is an endomorphism on G.

As an example of this corollary, let F be a commutative ring of finite characteristic and with a unity. Suppose that the characteristic $k = s(s-1)/2$ for some integer $s > 2$. Let G be the set of all ordered triples $\langle a, b, c\rangle$ over F with multiplication given by $\langle a, b, c\rangle\langle a', b', c'\rangle = \langle a + a', b + b', c + c' + ba'\rangle$. We have the well known class 2 group G of triangular matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ c & b & 1 \end{pmatrix}$$

where $Z = Q$ is the set of all $\langle 0, 0, x\rangle$. Since $\langle 0, 0, x\rangle^n = \langle 0, 0, nx\rangle$, the characteristic k is an exponent for Q. In general, $\langle a, b, c\rangle^n = \langle na, nb, nc + (n(n-1)/2)\, bc\rangle$ for each integer n. An easy calculation now shows that $(\langle a, b, c\rangle\langle a', b', c'\rangle)^s - \langle a, b, c\rangle^s\langle a', b', c'\rangle^s = \langle 0, 0, (s - s^2)ba'\rangle$. But $(s - s^2)ba' = -2kba' = 0$, so that $[s]$ is indeed an integral endomorphism of G.

BIBLIOGRAPHY

1. F. Haimo, *Groups with a certain condition on conjugates*, Canad. J. Math. **4** (1952), 369-372.

2. ———, *Power-type endomorphisms of some class 2 groups*, Pacific. J. Math. **5** (1955), 201-213.

3. W. Scott, *Group Theory*, Englewood Cliffs, New Jersey, 1964.

Received September 1, 1965. This research was supported jointly by the National Science Foundation and by Washington University under grants No. GP-89 and GP-3874.

WASHINGTON UNIVERSITY